Official Magazine of the
Defense Counterintelligence and Security Agency

Gatekeeper

Volume 1, Issue 4

IN THIS ISSUE

IN THIS ISSUE

VOL 1 | ISSUE 4

DCSA Gatekeeper

Published by the Defense Counterintelligence and Security Agency (DCSA) Office of Communications and Congressional Affairs (OCCA)

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil
571-305-6562

DCSA LEADERSHIP

William K. Lietzau
Director

Jon Eskelsen
Chief, OCCA

Cindy McGovern
Managing Editor

Elizabeth Alber
Editor

John Joyce
Staff Writer

Christopher P. Gillis
Staff Photographer

Halle Czechowski
Ashley Fancher
Ryan King
Cady Susswein
Monika Thomas

BARBARICUM
Layout, Editing, and Design

This Department of Defense (DOD) magazine is an authorized publication for members of DOD. Contents of the Gatekeeper Magazine are not necessarily the official views of, or endorsed by, the U.S. government, DOD, or DCSA. The editorial content of this publication is the responsibility of OCCA.

All pictures are DOD photos, unless otherwise identified.

FROM THE DIRECTOR

This month's cover story is about the National Center for Credibility Assessment or "NCCA." On October 1, we began a new fiscal year and NCCA formally transferred from the Defense Intelligence Agency (DIA) to DCSA in accordance with direction from the Under Secretary of Defense for Intelligence and Security (USD(I&S)).

NCCA is the federal center for credibility assessment, education, oversight, research, and development. NCCA supports 29 federal agencies, including multiple DOD organizations and warfighter elements, by providing initial education and training to certify federal personnel in credibility assessment (CA) technologies, a continuing education certification program for all federal agencies, and a Quality Assurance Program that develops, implements, and provides oversight for the federal CA programs. NCCA will be aligned under our Training Directorate, making our already extensive security education and training program even more robust.

This transfer is notable as the most recent major mission area to be transferred to DCSA. Just two short years ago, the National Background Investigations Bureau (NBIB) and DOD Consolidated Adjudications Facility (DOD CAF) merged with the legacy Defense Security Service (DSS) to become DCSA. Last year saw the formal transfer to DCSA of the National Background Investigation Services (NBIS) from the Defense Information Systems Agency (DISA), legacy IT systems from the Office of Personnel Management (OPM) as well as several programs from the Defense Manpower Data Center (DMDC). Each transfer presented a unique set of challenges, but the fact that we were able to accomplish them so successfully, while also bringing down the investigative inventory, meeting timeliness goals for investigations and adjudications, establishing a working capital fund, and continuing to deliver industrial security and counterintelligence support to industry, should be a source of pride for all DCSA employees. This was only possible because of the dedication of DCSA's workforce. I am proud to be part of such a professional team.

Now that this most recent transfer is complete, DCSA is turning its attention to transformation — how to best integrate these different missions and organizations into a cohesive whole that is greater than the sum of its parts. We need to do that to meet the increasingly complex challenges of today's security environment. Some of our plan to meet these challenges is described in another article on what we call the new Operating Model.

I recently had an opportunity to review and speak about DCSA's support to the new strategic plan for the Defense Security Enterprise (DSE). The strategy provides a framework for the DSE to elevate, integrate, and optimize defense security in the formidable threat environment of today. I believe the transfers mentioned above, and our continued transformation efforts underway, optimally position DCSA to implement this strategic vision for the Department and the larger U.S. government security community.

Thank you for reading, and thank you for your continued support to DCSA.

William K. Lietzau

William K. Lietzau

Director,
Defense Counterintelligence
and Security Agency

DCSA RECOGNIZES THE BEST IN INDUSTRIAL SECURITY

40 FACILITIES RECEIVE COGSWELL AWARDS IN 2021

On June 9, 2021, DCSA presented the annual James S. Cogswell Outstanding Industrial Security Achievement Award to 40 cleared contractor facilities during the virtual NCMS training seminar. The Cogswell Awards represent the "best of the best" of facility security programs that stand as models for others to emulate. These 40 facilities represent less than one-tenth of 1% of the approximately 12,500 cleared facilities in the National Industrial Security Program (NISP).

"Each of these recipients show clear management and corporate commitment for security," said DCSA Director William K. Lietzau during the virtual Cogswell ceremony. "But the facilities don't create excellent programs, people do — the facility security officers, the security staff, and the company leadership. Without their commitment and dedication, their facility would not be here today.

"While the focus and accolades today are justifiably on the Cogswell winners, I would be remiss if I did not also recognize the DCSA workforce — the industrial security representatives, the information systems security professionals, counterintelligence special agents, and others spread across the country in our field offices," Lietzau continued. "They are our first line of defense and the first number or email an FSO reaches for when there is a problem. And they are as committed to security excellence as the facilities we recognize today. Thank you all for your continued dedication."

To qualify, companies must establish and maintain a security program that exceeds basic NISP requirements. Recipients also help other cleared facilities establish security-related best practices, while maintaining the highest security standards for their own facility.

The Cogswell Award selection process is rigorous. A DCSA industrial security representative may only nominate facilities that have at a minimum two consecutive superior industrial security review ratings, which show a sustained degree of excellence and innovation in their overall security program management, implementation, and oversight. DCSA makes the final selections. Due to COVID-19 and the stand down of on-site security reviews, DCSA only considered facilities that had received consecutive superior ratings no later than January 1, 2018, for this year's Cogswell Award.

Established in 1966, the award honors Air Force Col. James S. Cogswell, the first chief of industrial security within the Department of Defense. Cogswell developed the basic principles of the industrial security program, which includes emphasizing the partnership between industry and government to protect classified information. This partnership provides the greatest protection for U.S. warfighters and our nation's classified information.

*The Cogswell Award is the most prestigious honor DCSA bestows on cleared industry. The numbers illustrate just how exceptional it is to achieve this status: Of the approximately **12,500** cleared facilities, less than one-tenth of 1% are selected annually to receive this award:*

Number of facilities awarded Cogswell honors by year

40	2021
60	2020
51	2019
39	2018
36	2017
42	2016
41	2015
40	2014
24	2013
26	2012
17	2011
9	2010
15	2009
23	2008
30	2007
29	2006
11	2005

CONGRATULATIONS TO THE 2021 COGSWELL AWARD WINNERS!

Alliant Techsystems Operations, LLC DBA: Northrop Grumman Systems Corporation
Northridge, CA

The Aerospace Corporation
Colorado Springs, CO

Azure Summit Technology, Inc.
Fairfax, VA

BioFire Defense, LLC
Salt Lake City, UT

Booz | Allen | Hamilton
Colorado Springs, CO

CNI Advantage, LLC
Norman, OK

CNI Global Solutions, LLC
Norman, OK

Corvid Technologies
Mooresville, NC

D.E. Technologies, Inc.
King of Prussia, PA

DRS Network & Imaging Systems, LLC
Cypress, CA

Eclipse Energy Systems, Inc.
St. Petersburg, FL

G&B Packing Co., Inc.
Jersey City, NJ

General Dynamics Mission Systems, Inc.
Florham Park, NJ

Iridium Satellite, LLC
Tempe, AZ

Leidos, Inc.
Albuquerque, NM

Lockheed Martin Advanced Technology Laboratories (ATL)
Arlington, VA

Lockheed Martin Rotary and Mission Systems
Akron, OH

L3 Harris Technologies, Inc.
Rochester, NY

MIT Lincoln Laboratory – Huntsville Field Site
Huntsville, AL

Mercury Systems, Inc.
West Caldwell, NJ

Mercury Systems, Inc.
Cypress, CA

Northrop Grumman Aeronautics Systems – El Segundo
El Segundo, CA

Northrop Grumman Systems Corporation, Platform and Mission Integration
Ocean Springs, MS

Northrop Grumman Systems Corporation
Sunnyvale, CA

Northrop Grumman Systems Corporation, Aerospace Systems Division
Melbourne, FL

Northrop Grumman Corporation – Launch Vehicles
Chandler, AZ

OnPoint Consulting, Inc.
Arlington, VA

Saab, Inc.
East Syracuse, NY

Sierra Nevada Corporation
Sparks, NV

Sierra Nevada Corporation
Folsom, CA

Scientific Research Corporation
Atlanta, GA

Smiths Interconnect, Inc.
Northampton, MA

Textron Systems Corporation (TSC)
Hunt Valley, MD

Torch Technologies, Inc.
Huntsville, AL

Undersea Sensor Systems, Inc.
DBA: Ultra Sonobuoy Systems
Columbia City, IN

University of New Mexico
Albuquerque, NM

Vertex Aerospace, LLC
Madison, MS

Viasat, Inc.
Germantown, MD

Viasat, Inc.
Marlborough, MA

Worldwide Language Resources, LLC
Fayetteville, NC

IN THEIR OWN WORDS

A representative sampling of the 2021 Cogswell winners were invited to share their formula for success with Gatekeeper readers. The following are tips and lessons learned on how to establish and maintain a high-quality security posture from facilities with proven track records.

ECLIPSE ENERGY SYSTEMS, INC.

By Jayne Zampelli, Security Officer

As a small business, becoming a James S. Cogswell Award recipient seemed like a near impossible achievement. We've faced many challenges along our journey to success, but an unwavering commitment to security coupled with direction and guidance from our DCSA partners paved the way. As the security officer, I'm honored to have been a part of this journey. With more than 25 years of security experience, I've established, managed, and inspected multiple security programs within both government and industry. Over the course of this time, there are a few key practices I've found to be vital to the overall success and enhancement of a security program:

- **Establish and sustain a security culture within the organization.** Leadership and management support are critical to this culture, but security awareness and education are the roots. Ensure that employees are aware of their security obligations and that they truly develop a strong understanding of them. Encourage employees to be a part of the culture by explaining the individual impact they have on the success of the security program and the impacts of poor security practices on the organization, their job, and ultimately national security. Everyone within the organization, regardless of position and security clearance level, including uncleared personnel, should recognize that security is a collective responsibility and commitment.
- **Do not measure the success of your security program strictly by your ability to check a box on a security checklist.** There are instances where we as security officers can technically check a box to show that we are compliant with a requirement, yet we are not effectively executing the intent of the requirement. For example, an inspection requires confirmation that procedures have been developed to safeguard classified material during an emergency, yet the inspection question does not measure the overall adequacy of the Emergency Action Plan (EAP), nor whether employees truly understand how to execute it. Self-inspections and DCSA inspections are an important tool for gauging the success of a program, but I believe that it is a security officer's responsibility to see beyond the confines of the checklist.
- **A security officer is much more effective when able to see the bigger picture of their security program.** Understanding how personnel security, information security, physical security, counterintelligence, insider threat, and other critical components of security interact and contribute to the success of the program creates a clear vision of how a program should look. It is not uncommon for a security officer to be more comfortable with one facet of security, overlooking others and creating an imbalance. Educating oneself on diverse and evolving security requirements better ensures that you are armed with the knowledge needed to fully orchestrate a well-rounded security program.
- **Don't be discouraged by the negative stigma that sometimes surrounds security.** Security can be perceived as an obstacle because it often presents challenges to day-to-day operations. Understanding the depth and impact of your security program and having a willingness to work towards solutions encourages positive collaboration amongst the team and helps incorporate security into business objectives.

We are truly honored to receive this award.

UNIVERSITY OF NEW MEXICO

By Deborah Kuidis, Facility Security Officer,
and Karen Brown, Assistant Facility Security Officer/Export Control Officer

Cleared universities are a unique challenge. Imagine a cleared defense contractor routinely operating with open doors, no badges, foreign visitors, and foreign research collaborations. These are just a few of the unconventional challenges that a facility security officer (FSO) of a cleared university and the DCSA industrial security representative (ISR) have to manage. Universities can't be clustered with industry so the security vulnerability assessment must be unique. Our security programs have the same goals, but we reach those goals in different ways. The following are just a few examples of how we reach our goals:

- **DCSA's Approach: We work with our ISR as a team when engaging with management and faculty to explain their role in relation to the university.** Sometimes, the engagement has to go beyond cleared personnel because research starts out unclassified but can quickly turn controlled unclassified information (CUI) or classified. If your ISR does not understand the complexities of how universities operate, the relationship could become contentious. For instance, our DCSA ISR finds ways to explain and justify questions about types of research and how it is being protected to avoid alienating our partnership with faculty. If the ISR is only looking for a "gotcha" moment rather than ensuring our security program goals are aligned to protect our nation's sensitive technology, everyone loses.
- **Awareness Training:** Don't give up on getting your message out there. Become immune to being called paranoid. Make it personal. What would the loss of research mean to faculty? For them, it's publish or perish and no patents.
- **Know Your Audience:** Tailor your terminology to your audience. If you use the term insider threat to uncleared professors and students, they will stop listening. Instead, use terms like risks and vulnerabilities. Focus your message on conduct, not nationalities. Faculty will never look at foreign collaborators as adversaries. Ask them: "When you are collaborating with a foreign national, who is doing all the talking? Is the collaboration a one-way street?" Make them concede the risks on their own and explain to you what their vulnerabilities are rather than the other way around. Then the important work of managing those risks can begin.
- **Support and Partnership:** It goes without saying that support from management is key. Ask relevant deans to be your advocate and introduce your ISR and counterintelligence special agent to them.
- **Academic Security and Counter-Exploitation (ASCE):** With increased oversight on universities by Congress, the ASCE Working Group was established in consultation with federal officials to help address the threat foreign adversaries pose to U.S. academic institutions. ASCE is coordinated by Kevin Gamache, chief research security officer, at Texas A&M University as a service to the academic community and works closely with key federal agencies such as DCSA, FBI, DOD, Department of State, and Office of the Director of National Intelligence (ODNI). FSOs and export control officers can request access to the listserv and Homeland Security Information Network portal to access quarterly newsletters, training, publications of effective practices, and information on the annual academic security conference.

In addition to our ISR Patricia Bourgoyne, we would like to express our gratitude to DCSA CI Special Agents Paul Godlewski and Nick Luce who taught us how to use our guts differently. It would have been impossible to receive two Cogswell Awards and the Award for Excellence in Counterintelligence in six years without this team.

L3HARRIS TECHNOLOGIES, INC.

By Richard Fiorella, Industrial Security Manager,
and Charles Marcera, Facility Security Officer

L3Harris Technologies is a proud member of the defense industrial community and has strong enduring relationships with DCSA and our customers. That association has facilitated a culture of security cognizance and business enablement illustrated in L3Harris' receipt of the Cogswell Award for the 17th straight year! This culture would not be possible without:

- **Senior Management Support:** Our level of success categorically starts with senior management support. Senior management sets the expectation with all of our employees that the standard for execution of our industrial security program is not only meeting government requirements but exceeding them. This support has been infused in the mindset of our employees and ensures the entire organization performs on a clear and consistent basis regarding governmental rules and regulations.

- **DCSA Partnership:** No organization has partnered more and kept our company on track as much as DCSA. We have built a strong partnership through many years of working together and promoting an information flow back and forth between our organizations. This cooperation strengthens our security program so that we can obtain the latest security requirements and intelligence threats to prepare for constant change.

- **Security Education:** Security, as expected, provides the day-to-day support that meets all requirements of the NISP. However, the security team must go beyond the minimum requirements for a successful security program. One key example of our security enhancements is a robust security education program. Not only does our company provide the required annual training, but we provide a monthly themed security education program throughout the year. This themed training concentrates on a specific topic each month and provides that information to employees through a variety of channels. From posters and electronic billboard messages to articles in our employee newsletters, all serve to drive home a singular, consistent monthly theme.

- **Self-Inspection:** Another positive initiative that enhanced our security program was a continuous self-inspection process. Sure, a once-a-year formal self-inspection will meet the minimum requirements, but it will not enhance your program. To augment the formal self-inspection, our company has set up a continuous DCSA-approved self-inspection process. Every month, the security team concentrates on a particular area within the industrial security program. This monthly look allows us to take a deep dive into a specific area and correct issues that may have been overlooked in a standard self-inspection process.

- **Employee Participation:** Finally, the absolute key to a robust security program is buy-in from employees. No program can be successful without their active participation. Our employees participate in numerous security training modules throughout the year and are well-versed on their security requirements. How do I know if our employees understand the requirements? Employee interviews, DCSA assessments, and a low number of security violations provide strong evidence that our employees actively recognize security requirements.

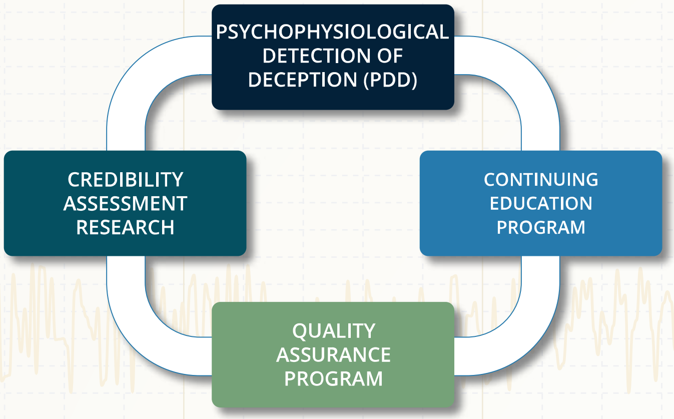
Senior management support, a strong DCSA partnership, and an engaged security team allows our employees to feel comfortable with following and reporting any security concerns.

NCCA TRANSFERS TO DCSA

Two years ago, on October 1, 2019, DCSA consolidated the Defense Security Service (DSS), National Background Investigations Bureau (NBIB), and the DOD Consolidated Adjudications Facility (DOD CAF). One year ago, the second wave of tranfers took place and the National Background Investigation Services (NBIS) transferred over in addition to legacy information technology systems from the Office of Personnel Management (OPM) and the Defense Manpower Data Center (DMDC). This October marks the move of the National Center for Credibility Assessment (NCAA) from the Defense Intelligence Agency (DIA) to DCSA. While it is the smallest of the three transfers with roughly 75 government and contractor employees, this move is no less significant, bringing a unique mission and capability to DCSA and the Training Directorate.

NCCA's mission is to conduct credibility assessment training and education, research and development, technical support, and oversight activities for federal polygraph and credibility assessment mission partners.

NCCA training supports nine DOD and 21 other federal agencies. Its premier course is the Psychophysiological Detection of Deception (PDD) course, held three times per year in residence. This course provides the initial skills to prepare students for a polygraph career within the federal intelligence, security, and law-enforcement communities. This graduate-level program consists of courses in psychology, physiology, and research methods, as well as polygraph history, theory, and methodology. Realistic scenario-based practical exercises are conducted throughout the program to provide students with hands-on instruction in polygraph techniques and instrumentation.


PSYCHOPHYSIOLOGICAL DETECTION OF DECEPTION (PDD)
CREDIBILITY ASSESSMENT RESEARCH
CONTINUING EDUCATION PROGRAM
QUALITY ASSURANCE PROGRAM

The Continuing Education Program, established in 1996, requires federal examiners to attend a minimum of 80 hours of continuing education every two years. This educational requirement can be met through attendance at NCCA-approved professional seminars, or with any of the 26 continuing education courses taught at the NCCA campus and other locations.

NCCA's Quality Assurance Program ensures federal agencies comply with all applicable federal polygraph program policies, practices, and procedures. Finally, NCCA is known for its credibility assessment research and participation in various polygraph research studies and providing peer reviews of research proposals.

> "NCCA's addition to the DCSA Training Directorate further enhances the directorate as a complementary and integral component that elevates the security readiness posture of individuals who have crucial roles to perform in assuring and maintaining the security of our nation. The reputation that we desire for ourselves is one of being active participants in the noble objective, which entails far more than being thought of as simply a collection of schoolhouses."
>
> — Kevin J. Jones, Director, Training Directorate

THE ORIGIN AND EVOLUTION OF NCCA

1951 U.S. Army Polygraph School established as part of the Provost Marshal General School at Fort Gordon, Georgia, to provide education on the operation of the polygraph and other credibility technologies.

1962 Provost Marshal School redesignated as the U.S. Army Military Police School (USAMPS) and Army Polygraph School remains under its auspices.

1975 USAMPS and the polygraph school are transferred to Fort McClellan, Alabama.

1985 Congress passes bill directing the secretary of defense to institute a program of counterintelligence polygraph examinations for military, civilian, and contractor personnel whose duties involve access to classified and highly sensitive compartmented information.

1985 Deputy secretary of defense signs memorandum designating the secretary of the Army as executive agent for polygraph training within DOD.

1986 USAMPS Polygraph School realigned and designated as the DOD Polygraph Institute (DODPI). It is transitioned from a vocational and technical polygraph training school to an educational institution.

1991 Secretary of the Army executive agency responsibility is eliminated and the authority, direction, and control of DODPI is transferred to the assistant secretary of defense for command, control, communications, and intelligence.

1993 Joint Security Commission is formed to address security concerns within the federal government. It recommends 1) consolidating the CIA Polygraph School with DODPI to form a single polygraph institute and that 2) DODPI be the executive agent for a robust, interagency-coordinated research program.

1999 Operational responsibilities for DODPI placed under the Defense Security Service (DSS), the precursor to DCSA. As part of the Base Realignment and Closure (BRAC) in June, DODPI moves to its present location at Fort Jackson, South Carolina.

2002 DODPI functionally transferred from DSS to the newly established Counterintelligence Field Activity (CIFA). On October 1, 2003, DODPI falls under operational control of CIFA.

2003 DODPI is accredited by the Accrediting Council for Independent Colleges and Schools to award a certificate of graduate study in the psychophysiological detection of deception. Several universities now accept the program's coursework for graduate credit.

2007 Deputy secretary of defense signs a directive renaming DODPI the Defense Academy for Credibility Assessment (DACA), a name representing the full spectrum of credibility assessment missions.

2008 DACA transitions under the operational control of the Defense Intelligence Agency (DIA).

2010 Undersecretary of defense for intelligence recommends redesignation of DACA as NCCA to give it congressional recognition as a national center and a clear focal point as the leader for federal credibility assessment issues. Recommendation is approved by the deputy secretary for defense.

2012 Director of National Intelligence James Clapper endorses NCCA as "the office of primary responsibility across the executive branch for polygraph examiner education and training, continuing education certification, the quality assurance program, and credibility assessment research."

2020 Undersecretary of defense for intelligence and security (USD(I&S)) directs a realignment of NCCA from DIA to DCSA to align with DCSA's role as the functional manager for DOD security education, training, and certification. NCCA begins a phased transfer to DCSA with full resource alignment scheduled for Fiscal Year 2022.

DCSA'S TRANSFORMATION: BECOMING ONE ENTERPRISE

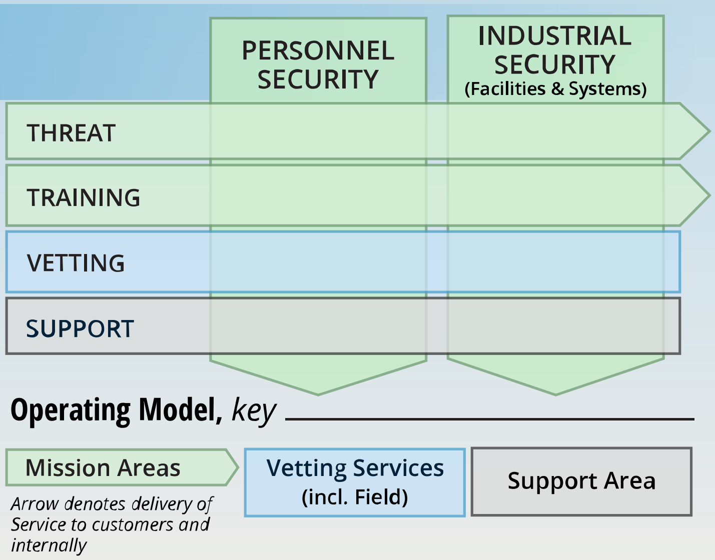
By Nicoletta Giordani
Chief Strategy Officer

The article is a follow up to "**DCSA Operating Model: Uniting the Agency in Achieving its Vision**" in the January 2021 Gatekeeper, which unveiled the concept for the DCSA Operating Model.

Shortly after its standup in October 2019, DCSA began work on a new Operating Model (OpModel), an articulation of how DCSA must operate in the future to deliver mission value. The new model defines how core missions and supporting operations come together to optimize mission performance and customer service through increased use of risk-management approaches, empowerment through technology and data, and scaling of enabling support to meet evolving mission needs. Right now, DCSA is moving into closer alignment with the new OpModel concept with over 45 transformations across the agency. The following are some key examples, highlighting their impacts on the agency and its stakeholders.

BUILDING A COMMON OPERATING PICTURE OF RISK INFORMATION

With multiple security missions coming together under DCSA, the agency OpModel prescribes more integration between mission sets — more communication, coordination, and a shared situational awareness of risks. To enable this, DCSA introduced a security risk management capability to provide a more holistic view of vulnerabilities, threat, and consequence information across the agency through enhanced analytics and case management abilities. A cross-agency team reviewed current DCSA threat and vulnerability activities for overlap and opportunities for sharing and coordination. The team also defined central components to an integrated Information Technology (IT) capability that supports vulnerability and threat information sharing across mission sets, incorporating risk frameworks and leading industry practices that build a common operating picture. The next step is to develop and execute a roadmap that will define policies, processes, and resources for effective implementation as well as technology requirements, which may include a platform that connects DCSA's existing IT systems.


PERSONNEL SECURITY
INDUSTRIAL SECURITY (Facilities & Systems)
THREAT
TRAINING
VETTING
SUPPORT
Operating Model, *key*
Mission Areas
Arrow denotes delivery of Service to customers and internally
Vetting Services (incl. Field)
Support Area

OPTIMIZING THE FIELD

The rapidly changing threat environment demands that DCSA operate in a more integrated fashion in the field. The Chief Strategy Office (CSO) is working closely with stakeholders across the Background Investigations (BI), Critical Technology Protection (CTP), and Counterintelligence (CI) mission areas to build an integrated field workforce. Aligning legacy field organizations into one structure and standardizing common field processes and procedures will enhance cross-mission information sharing, prioritization coordination, and cultural integration.

Ushering in a Cohesive Field Structure. DCSA is standing up a new regional structure to improve integration and communication across the field. The legacy National Background Investigations Bureau (NBIB) included three regions, while legacy Defense Security Service (DSS) was divided into four. The new structure merges all field mission areas into a single four-region structure: Western, Central, Eastern, and Mid-Atlantic. The consolidation of the field under an integrated DCSA field structure will be effective on October 1, 2021.

Key Reimbursement Process Enhancements. CSO and BI are preparing to pilot an automated process for the submission and reimbursement of BI field agent expenses, ultimately making this important process easier and faster for the field. This transformation will allow personnel to obtain investigative information more easily, without risking long-term delays in reimbursement for out-of-pocket expenses. Once implemented, the team estimates a 63% time savings, totaling approximately 7,000 saved hours per year, based on a time-in-motion assessment of the current process.

EVOLUTION OF THE ENABLING SUPPORT FUNCTIONS

Consistent with the OpModel, DCSA is building an Enterprise Service Delivery (ESD) platform to provide exemplary service to the mission directorates. The ESD platform will ultimately be a single, cross-functional information technology capability that will deliver service management and internal customer relationship capabilities for critical functions such as hiring and onboarding processes. Using a common DCSA-centric IT platform will support agency-wide self-service requests; provide transparency into delivery processes through clear and automated workflow tracking; reduce manual tasks, processing time, and email-based management of agency wide service delivery; and provide improved controls, process accuracy, and reporting capabilities.

Industry research suggests that organizations can improve customer experience by increasing responsiveness, workforce capacity, internal controls, productivity, and transparency through improved service delivery. Building this capability through a service delivery platform in other agencies has been demonstrated to provide a 10-15% annual productivity improvement for service consolidation, 25% increase in contract transactions processed, and over 90% decrease in invoice processing.

Next steps. DCSA validated a customer service vision for ESD and selected a technical capability that will be deployed across the agency. Currently, the Program Executive Office (PEO), CSO, and the Human Capital Management Office (HCMO) are piloting an onboarding component of ESD that includes tracking hiring actions with near real-time reporting capabilities. In the future, DCSA will expand this service delivery capability to other enabling functions and mission areas proliferating ease of use and transparency benefits throughout DCSA.

HARNESSING THE POWER OF DATA

Alignment with the OpModel requires a mastery of enterprise data — both in how it's managed and analyzed. DCSA has access to millions of data points that can inform operations to support more evidence-based decision making. Transformations to DCSA's enterprise data management, analytic, performance measures, and reporting capabilities will enable evidence-based, data-driven decision making across the agency. The Chief Data Office (CDO) initiated several data-focused transformation projects in collaboration with DCSA's organizations:

- **The DCSA Data Strategy**. DCSA is preparing to unveil and implement a data strategy to transform the agency into a data-centric organization that postures DCSA to manage data as an enterprise asset. DCSA exerts tremendous effort to plan and use traditional strategic assets (e.g., people, finances, technology, and facilities) to optimize mission effectiveness and efficiency. In the same manner, DCSA's data is a strategic asset — a high-interest commodity that must be leveraged to bring immediate and lasting advantage over the wide-ranging threats DCSA regularly encounters and mitigates. For an agency to be successful, it must manage its data assets effectively and consistently.
- **Governance for strategy implementation**. To scale data governance and transformation in a collaborative way, DCSA stood up the Data Stewards Council (DSC), a decision-making body overseeing the agency-wide stewardship of DCSA data assets. The DSC is comprised of representatives from all mission and support areas, ensures DCSA's strategic data assets are safeguarded appropriately and available to authorized personnel and mission partners to meet mission needs in compliance with applicable laws, regulations, and policies.
- **Scaling data-driven Insights**. CSO is incubating predictive analytic capabilities that can be expanded across mission areas and enabling support functions to optimize processes like financial forecasting, adjudications workload management, and Trusted Workforce impacts on personnel security mission workload. This transformation will provide DCSA with a more comprehensive understanding of its operations and the degree to which the agency continues to fulfill its mission and vision.

REACHING OUR FUTURE STATE

OpModel implementation is ultimately about equipping DCSA with the processes and tools of tomorrow. Progress has been made across the mission areas in just this year, but transformation is an ongoing journey, shaping small- and large-scale changes that will take years to come to fruition. As the agency continues to move forward, it will require collaboration and integration — linking process experts, transformation specialists, and project managers to modernize how the agency does business.

BE CYBER SMART: LEVERAGE AVAILABLE RESOURCES AND TOOLS TO BE MORE SECURE ONLINE

By Roxanne Landreaux
Office of the Chief Information Officer

Cybersecurity Awareness Month, now in its 18th year, is a joint effort of the Cybersecurity and Infrastructure Agency (CISA) and the nonprofit National Cyber Security Alliance. It is held each October to ensure all Americans have knowledge of the resources and tools available to be safer and more secure online. The theme for 2021 is **"Do Your Part. #BeCyberSmart."**

In addition to raising awareness about cybersecurity, this is also an ideal time to amplify leadership and employee roles and responsibilities in an organization's effort to create and maintain a cyber-secure culture — especially in today's increasingly digital and hyper-connected environment. It is also an opportunity to practice good cybersecurity practices at home on personal devices.

To that end, take some time during October to communicate and practice cybersecurity in ways that promote a cyber-secure culture that maximizes employee productivity and satisfaction to facilitate business continuity.

Cybersecurity awareness activities can include fun and educational efforts that seek to increase knowledge, reinforce security behaviors, and provide accessible resources in order to educate all users of the effective strategies that can keep them and others secure. Activities may include practicing:

- Protecting data
- Avoiding pop-ups, unknown emails and links
- Using strong password protection and authentication
- Connecting to secure Wi-Fi
- Enabling firewall protection at work and home
- Investing in security systems
- Installing security software updates and back up files
- Embracing education and training

A cyber-secure culture is an ever-evolving shared responsibility that is integral to ensuring organizations meet and exceed mission needs, fulfill stakeholder expectations, and achieve the ongoing efficacy of the organization and the nation.

As a part of the month's activities, Cybersecurity Career Awareness Week is October 18-23 and is designed to increase awareness of the important role that cybersecurity personnel play in keeping organizations safe, as well as the job opportunities in the field.

While most of us bring focused attention to cybersecurity best practices this month, the routines you set during this time should continue throughout the year. Connecting securely is a choice we must all make every day. In today's world the internet touches nearly every aspect of our daily lives. When we all take steps to secure our connected devices, our data, and ourselves, we all benefit.

More information on the #BeCyberSmart campaign is available at www.dhs.gov/be-cyber-smart.

DCSA MARKS 10-YEAR ANNIVERSARIES AT THE RUSSELL-KNOX BUILDING AND FORT MEADE

Base Realignment and Closure (BRAC) in 2005 directed the construction of two facilities that DCSA continues to call home: one at Fort George G. Meade, Md., and the other (DCSA Headquarters) at Marine Corps Base Quantico, Va. Both buildings just marked 10 years since their ribbon cuttings.

The first BRAC recommendation (130) mandated that the Defense Security Service (DCSA's legacy organization) close the Defense Industrial Security Clearance Office (DISCO) in Columbus, Ohio, and relocate it to Fort Meade, where the DOD's 10 Central Adjudicative Facilities (CAFs) were co-located. This move also included the CAFs from the Army, Navy, Air Force, Joint Chiefs of Staff, National Security Agency (NSA), Defense Intelligence Agency (DIA), National Geospatial Intelligence Agency (NGIA), Washington Headquarters Service (WHS), and the Defense Office of Hearings and Appeals (DOHA). In 2012, the Deputy Secretary of Defense directed the functional consolidation of the military service CAFs with DISCO, WHS, and the Joint Chiefs of Staff, resulting into the Department of Defense Consolidated Adjudications Facility (DOD CAF), as we know it today.

Digital rendition of the Fort George G. Meade building.

Aerial view of the construction site for the Fort George G. Meade building in Maryland.

Ribbon cutting ceremony for the Fort George G. Meade building.

Construction of the new 150,000 square foot building began in 2009 and was designed for 770 employees, including 137 authorized spaces for DSS. The ribbon was cut on the new building on August 17, 2011, a month before its September 15 deadline.

The second recommendation (131) mandated DSS close its headquarters located at Braddock Place in Alexandria, Va., and relocate to Marine Corps Base Quantico, where it would be co-located with five agency headquarters elements, including the Air Force Office of Special Investigations (AFOSI), Naval Criminal Investigative Service (NCIS), Army Criminal Investigations Division (CID), and Defense Intelligence Agency (DIA) counterintelligence operations.

Construction of the new building, known as the Russell-Knox Building (RKB), began in September 2008, removing over 615,000 cubic yards of earth, pouring over 30,000 cubic yards of concrete, and planting over 1,200 new trees within the compound. A ribbon cutting ceremony was held on September 19, 2011. RKB was originally designed to hold approximately 2,700 personnel within the 720,000 square foot structure, and 374 spaces were designated for DSS employees. The agency quickly outgrew this space, and in 2013, DSS began construction of a 40,000 square foot addition to RKB that is now home to DCSA headquarters personnel.

Digital rendition of the RKB.

Aerial view of the RKB construction site.

Wall being constructed around the RKB.

Ribbon cutting ceremony for the RKB.

HOW WAS THE RUSSELL-KNOX BUILDING AND ROAD NAMED?

THE BUILDING

In a contest to name the facility, NCIS proposed naming it after two pioneers in creating a modern counterintelligence arm in the Department of the Navy — Marine Corps Major General John H. Russell, Jr., and Navy Commodore Dudley Wright Knox.

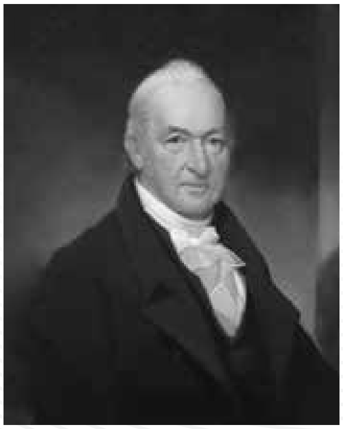
Maj. Gen. John H. Russell, Jr.

Commodore Dudley Wright Knox

MAJ. GEN. JOHN H. RUSSELL, JR. (1872–1947) was the 16th Commandant of the Marine Corps and a key player in the development of modern counterintelligence. A graduate of the U.S. Naval Academy, he served from 1894 to 1936 in the U.S. Marine Corps. Russell served aboard the USS Massachusetts during the Spanish-American War and received the Distinguished Service Medal and the Navy Cross, among other awards. After the war, he commanded Marines at a number of stations in Guam, the Panama Canal Zone, China, Honolulu, Annapolis, and Washington, DC.

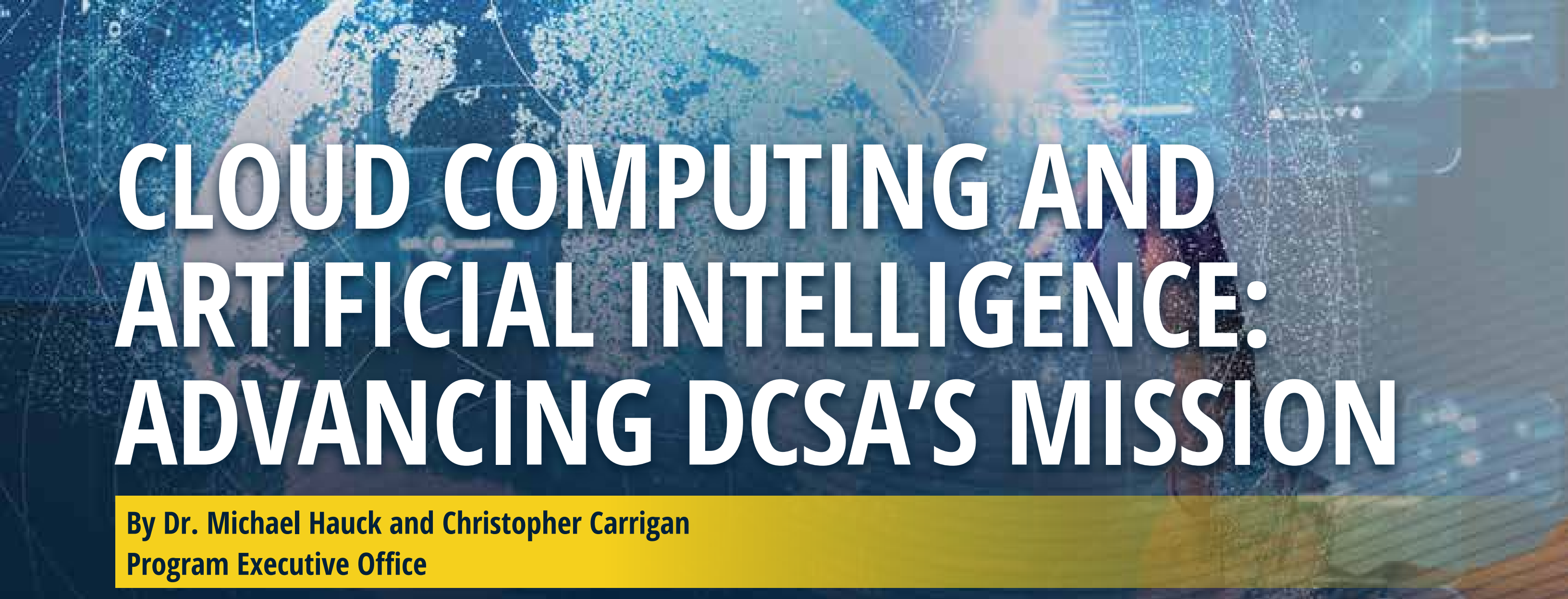
COMMODORE DUDLEY WRIGHT KNOX (1877–1960) graduated from the Naval Academy in 1896 and served aboard a number of ships. During the Philippine Insurrection, he commanded the gunboats USS Albay and USS Iris. He commanded three of the Navy's first destroyers before commanding the First Torpedo Flotilla. Russell served with the Office of Naval Intelligence (ONI) from 1913 to 1917. Following his ONI assignment, he was dispatched to the Dominican Republic and Haiti. Upon his return to the United States in 1930, he was assigned as Commanding General, Marine Corps Base, San Diego, and then to Marine Barracks, Quantico, Va. He was appointed Commandant of the Marine Corps in 1934 and remained in that position until his retirement in 1936.

HOW DID THE TWO MEET? In 1913, on the eve of World War I, Russell was assigned to the ONI, and the following year, Knox also reported there. With a wealth of political and military machinations brewing overseas, the ONI was given the added responsibility of investigating alleged espionage and sabotage. The two officers joined forces to develop an organic capability within the Department of the Navy to conduct such investigations. A plan to reorganize ONI was developed, but it found little favor until the so-called "Black Tom" incident of July 1916, when an explosion at a Jersey City munitions dock resulted in some $40 million in damage. The blast was blamed on German saboteurs and dramatically accelerated the effort to generate a counterintelligence and investigative capability within the Navy. The result was the creation of a Naval District Information Service. Counterintelligence units assigned to naval district were collectively designated the "Naval Secret Service." Undercover "branch offices" were opened in major American maritime centers. By the end of the war, some 18 German spies were reportedly identified by these naval counterintelligence units.


Benjamin Tallmadge

THE ROAD

In addition to naming the building, the contest also included the road leading into RKB. AFOSI suggested "Tallmadge Road" in honor of Benjamin Tallmadge, who served as a colonel and head of the Continental Army Intelligence during the American Revolution. Tallmadge organized a spy ring, referred to as the Culpepper Gang, in British Occupied New York for General George Washington. He was also a key figure in disclosing the espionage of British Major John Andre and U. S. Major General Benedict Arnold. After the war, Tallmadge served in the U.S. House of Representatives from 1801-1817.



CLOUD COMPUTING AND ARTIFICIAL INTELLIGENCE: ADVANCING DCSA'S MISSION

By Dr. Michael Hauck and Christopher Carrigan
Program Executive Office

DCSA's missions are expanding and transforming in response to an evolving threat landscape and related national policy shifts. As the threats and policies evolve, so do the technologies that enable the agency to stay ahead of its adversaries. Cloud computing and artificial intelligence (AI) are two classes of technology in use that will enable DCSA to be a better gatekeeper at protecting America's critical technology, vetting personnel, countering foreign intelligence, and mitigating insider threat.

WHAT IS THE CLOUD?

The cloud is a secure capability that resides in commercial facilities with DOD-level data protections, which provide DCSA the ability to cost-effectively access large sets of data, however they are stored. The DCSA cloud operating environment not only provides efficiencies and economies of scale for large data processing and analytics, it also fortifies the protection of the agency's most critical business asset: data — the same data that DCSA is entrusted to protect and defend.

Cloud technology supports Continuity of Operations Planning (COOP) by providing redundant, off-site failover for critical systems. It allows for more secure cyber protection protocols through different ways of using encryption and separate cloud security solution providers. It also sets the framework for the agency to better manage, control, and process data at scale and speed. The DCSA cloud infrastructure includes a number of built-in platforms and applications that are intended to make it fast and easy to add new mission systems as mission and requirements change. These include Big Data Platform (BDP) and a special data brokering architecture. The BDP provides a base set of programming tools to build computer applications, while the data broker manages the flow of data according to policy. Both support the implementation of AI tools and functions.

WHAT IS ARTIFICIAL INTELLIGENCE?

Artificial intelligence (AI) refers to the ability of machines to perform tasks that normally require human intelligence — things like recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action. How do we make a computer act as if it were intelligent? Alan Turing, who many consider to be the father of artificial intelligence, argued that any general-purpose computer could be programmed to mimic the human brain if it were powerful enough. He wrote, "If we wish to imitate anything so complicated as the human brain, we need a very much larger machine than any of the computers at present available [in 1951]."   Today's computers — even cell phones — are powerful enough that machines beat humans at chess and some aircraft can fly themselves.

Most Americans are already accustomed to interacting with AI technology. If your car has a lane-keeping function, anti-lock brakes, or can self-park, then AI has been your co-pilot! If you have received movie recommendations on Netflix or purchase suggestions from Amazon, then you know how effective AI can be at assessing your likes and dislikes. And, if you have watched a Major League Baseball game lately, the coach likely picked the lineup with the aid of AI algorithms.

WHAT IS AN AI ALGORITHM?

An algorithm is computer code (or a set of instructions for the computer) that implements logic, business rules, relationships among things, and other mathematical

functions to solve problems. Humans trained in programming languages can write algorithms or, believe it or not, computers can too! It is important to note that as DCSA develops AI algorithms, we build them in accordance with DOD's AI ethical framework. This framework requires DCSA's AI programs to be responsible, equitable, traceable, reliable, and governable. DCSA ensures its AI models are explainable, tested, accurate, and backed by scientific data, and includes mechanisms to detect potential bias or algorithm deviation.

HOW DOES DCSA USE AI ALGORITHMS?

Just like automobile makers, online stores, and sports teams, DCSA leverages AI to solve business problems and improve customer service. AI enables DCSA to increase the depth and breadth of background investigations, improve the quality of analytic products, increase consistency in adjudications, and detect risk more effectively. DCSA seeks to use AI to provide actionable information in the right context at the right time to support human decision makers, while ensuring context is consistent with the same standards and guidelines humans use to make decisions today. The use of AI is intended to augment human decision (not replace) by making it easier to identify critical information from large voluminous data sets.

WHAT IS DCSA DOING TO BUILD A FOUNDATION THAT LEVERAGES THESE TOOLS?

The DCSA Program Executive Office (PEO) has developed a foundational framework that relies on both cloud computing and AI technologies. The PEO's Cloud Services and Data Management (CSDM) Program Office and experts from the PEO's Architecture, Engineering, and Data Science team play a critical role in setting the foundation for technology modernization and digital transformation of agency systems into secure, modern, cloud and AI-enabled platforms. These efforts allow DCSA to operate its Continuous Vetting (CV) mission at scale. Today, there are approximately 3.2 million individuals enrolled in CV, which leverages automation and commercial and government data sources to enable the transformation of the personnel vetting program as DCSA implements the Trusted Workforce 2.0 strategy. Similar capabilities underpin the Critical Technology Protection (CTP) mission as it evaluates risks associated within the facility security clearance program.

Through partnerships with leading DOD research and technology laboratories, the PEO developed an operational pilot that aims to improve the quality of personnel security decisions. At high speed, it combs through large sets of data to detect variance in the DOD Consolidated Adjudications Facility (CAF) outcomes. At full maturity, the project will bring additional efficiencies as it learns from prior adjudications. It will prioritize and distribute workload, detect missing information, and visualize critical data elements.

Today we click through folders, sift through files, and sort through spreadsheets. Tomorrow, AI tools will reduce manual repeatable processes, provide rapid and consistent insight, and create intelligent systems to keep pace with the changing world. The AI-powered cloud optimizes operations, transforms services, and empowers the workforce. Translating this scale into impact and bringing cloud computing and artificial intelligence to the organization as a commodity capability will enable DCSA to maintain pace with its national security strategy.

NITAM 2021 FOCUSES ON CULTURAL AWARENESS, INSIDER RISK, AND HELPING PEOPLE BEFORE INCIDENTS OCCUR

By John Joyce
Office of Communications and Congressional Affairs

Given today's global environment and focus on cultural and social awareness in the workplace, it was only natural that cultural awareness was the theme of 2021's National Insider Threat Awareness Month (NITAM), celebrated this September.

As part of the month's activities, Department of Defense (DOD) and federal employees were asked to develop videos highlighting their organization's daily actions to create a positive workplace culture. The videos focused on how these organizations create a workplace culture based on respect and understanding of its diverse workforce — one that avoids social missteps, increases engagement, values diversity, and reduces the risk of insider threats.

Organizers of NITAM, a collaborative effort between DCSA, the National Counterintelligence and Security Center (NCSC), National Insider Threat Task Force (NITTF), the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)), and the Department of Homeland Security (DHS), then used the video competition to highlight the impact that cultural awareness has on safeguarding the United States from the risks posed by insider threats.

DOD Insider Threat Management and Analysis Center (DITMAC) Acting Director James Shappell reflected on the link between workplace culture and insider threat, "The topic of cultural awareness, and the theme of NITAM 2021, is one that's been front and center over the last year. Many of us faced major changes in the work environment, some of us became isolated, and we witnessed major cultural movements in our country," said Shappell. "From an insider threat perspective, I think it's important that we make strong efforts to contextualize behaviors we see based on the culture of organizations and the people within, to challenge our assumptions and bias, and think again about situations where we may have rapid and natural inclinations to draw biased conclusions."

"This can be challenging when looking at available information from pillars such as security, law enforcement, counterintelligence, and human resources," acknowledged Shappell. "Part of our job is to have that holistic view and that absolutely includes things like cultural impacts and influences, as well as cultural nuances of individuals."

In addition to its focus on increasing cultural awareness, this year's NITAM was designed to enhance the ability of programs across DOD and federal agencies to detect, deter, and mitigate insider threats and promote reporting. Insider threat awareness prevents the exploitation of authorized access to cause harm to an organization or its resources. It is vital to prevent these actions and safeguard national security while protecting privacy and civil liberties. However, insider threat as a mission, and as a specialty, remains a relatively new concept.

“The original concept of insider threat made sense,” Shappell recounted, “but we’ve really started to work toward understanding the types of reporting we receive and how we interact with the pillars of the program and the people in our organization. It really feels like we are, smartly, moving toward insider risk.”

In other words, the counter-insider threat community is transitioning toward helping people before an issue escalates or moves in the wrong direction. “To get there and be most effective, we need to remove the stigma of reporting,” said Shappell. “Leaders view the words ‘threat’ and ‘risk’ very differently. We can help by emphasizing that as insider threat professionals, we are here to assist with risk-based decisions and support individuals who may be headed down a path. Our goal is to get them on the right path. Ideally, we want to engage individuals before an issue becomes a threat.”

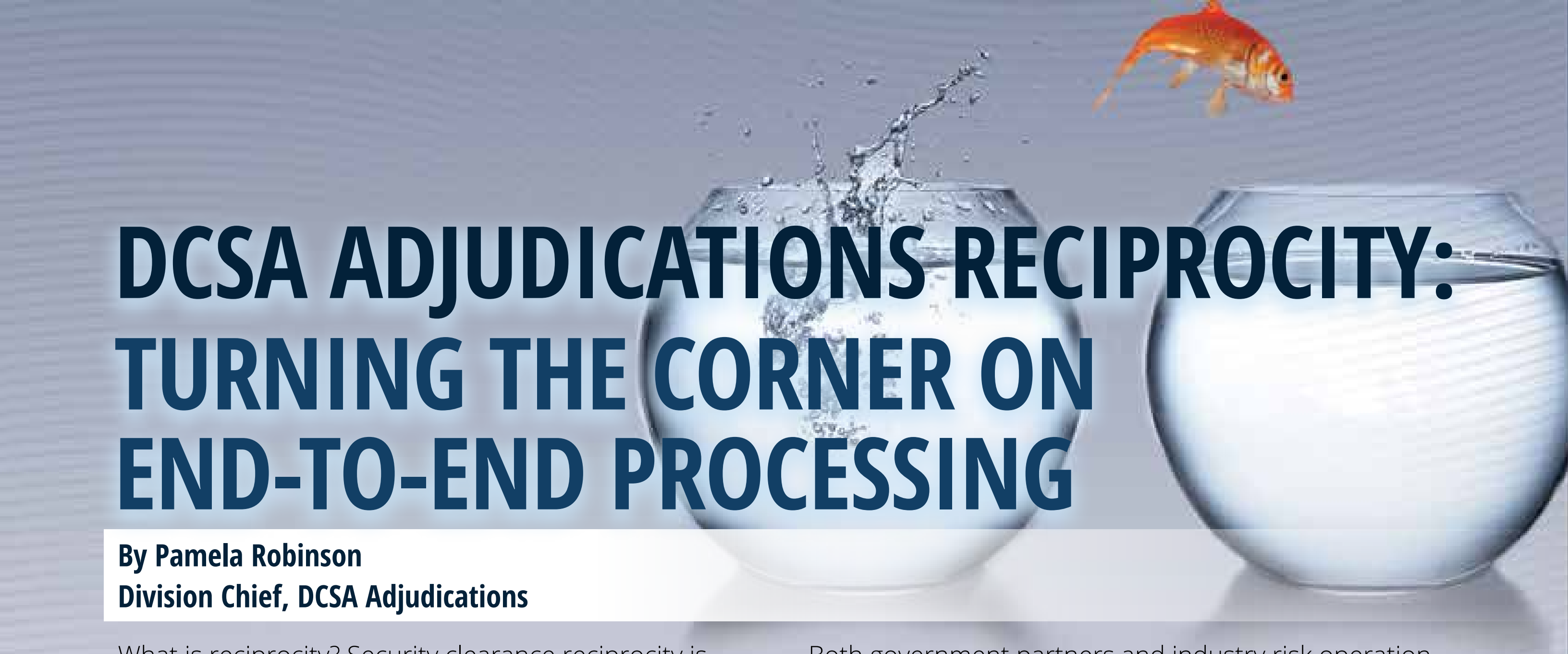
That engagement can happen when a workplace culture prioritizes a collective understanding of different backgrounds and cultures, mutual respect towards one another, and continued education on diversity and inclusivity in the workplace. Consequently, individuals and organizations achieve higher cultural competence through cultural awareness to mitigate insider risk.

Shappell notes that communicating the good the insider threat program can do (beyond stopping people with malicious intent) and driving that value proposition to leaders will continue to improve the support for their efforts. “We seem to remain on the right path in our efforts to increase reporting in areas of concern and trying to increase overall awareness of the workforce,” said Shappell. “What will be critical for our insider threat hubs and professionals moving forward will be finding the right way to receive that information while providing direct support to leaders or on referring action to our pillars to continue to demonstrate value-added.”

In all, NITAM 2021 topics encompassed vigilance, safety, security, the counterintelligence threat, recognizing and reporting indicators, the proactive nature of insider threat programs, respect for privacy and civil liberties, and differentiating between legitimate whistle blowers and inside threats.

“NITAM is a great opportunity to spotlight the efforts of the insider threat mission, but it can’t be the single time each year we think about, talk about, and focus on how we improve reporting to insider threat hubs and maximize the value in helping people find the right pathway when they are facing difficulties or challenges,” said Shappell. “NITAM must be a springboard each year into how we improve the insider threat mission and demonstrate the value of our efforts. From our perspective at DITMAC, we will strive to continue to be a value-add to the community and broadly support the efforts of the Department of Defense.”

The video producers, including competition winners, were recognized during the third annual Virtual Insider Threat Conference and each winner communicated the 2021 NITAM theme of “Insider Threat and Cultural Awareness.” Winners showed creativity, emphasizing that awareness and understanding of cultural differences within a workforce helps organizations and individuals prevent unintentional harm that can lead to an increased risk of insider threats. All of the entries are featured on the NITAM 2021 website (www.cdse.edu/itawareness), in digital and print publications across DOD, and on the free Insider Threat Sentry mobile app.



DCSA ADJUDICATIONS RECIPROCITY: TURNING THE CORNER ON END-TO-END PROCESSING

By Pamela Robinson
Division Chief, DCSA Adjudications

What is reciprocity? Security clearance reciprocity is the process where clearances are transferred between agencies. As defined in the Director of National Intelligence's (DNI) Security Executive Agent Directive (SEAD) 7, Reciprocity of Background Investigations and National Security Adjudications, reciprocity is:

- The acknowledgement and acceptance of an existing background investigation conducted by an authorized investigative agency,
- The acceptance of a national security eligibility adjudication determined by an authorized adjudicative agency, and,
- The acceptance of an active national security eligibility determination granted by an executive branch agency.

In short, SEAD 7 establishes requirements for reciprocal acceptance of background investigations and national security adjudications between agencies and directs determinations be made within five business days of receipt of an agency's personnel security program.

Note: Processing for employment, suitability, or fitness requirements is considered outside the scope of national security reciprocity determinations and is not counted or reported as part of the security processing to make a national security reciprocity determination.

Both government partners and industry risk operational readiness when employee reciprocal clearances are delayed. Approximately 80-90% of reciprocity requests are from cleared industry who may experience financial impacts if unable to start employees in a timely manner.

Prior to January 2020, reciprocity determination timeliness averaged 65 days end-to-end, well above the SEAD 7 requirement of five days. A Lean Six Sigma study conducted within Adjudications from January to May 2020 examined the reciprocity process for Adjudications. The study identified opportunities for improvement by both mission areas to eliminate bottlenecks and ultimately reduce timelines to achieve SEAD 7 compliance.

DCSA Adjudications fully implemented the Lean Six Sigma recommendations in June 2021 and is now consistently meeting SEAD 7 timeliness for end-to-end reciprocity request processing. That month, DCSA Adjudications processed and concluded reciprocity actions in an average of two days end-to-end — a 97% improvement over January 2020 performance.

DCSA has made great strides to advance the efficiency of the DOD personnel security program. The foundation of this effort is ensuring that DCSA is at the forefront of clearance and access reciprocity with regard to all DOD civilian, military, and contractor personnel. Reciprocity process improvements within Adjudications has significantly improved the operational readiness for government and industry partners.

LAW ENFORCEMENT LIAISON OFFICE ADVANCES CRIMINAL HISTORY RECORD INFORMATION ACCESS

By Daniel Leary, Executive Program Manager
Background Investigations Customer Service Enterprise (CSE)

Ensuring a workforce worthy of trust from the American people requires identifying potential risks that are critical to understanding the "whole person." This includes criminal activity or adverse encounters with law enforcement at the federal, state, local, and tribal levels, as well as court actions. This data, collectively called Criminal History Record Information (CHRI), is often difficult to access, which poses an ongoing challenge to the federal personnel vetting mission. DCSA's Law Enforcement Liaison Office (LELO), which falls under Background Investigations, works tirelessly to overcome this challenge and ensure access to the best, most accurate, and complete information.

In an effort to address CHRI challenges, the National Defense Authorization Act (NDAA) for Fiscal Year 2014 directed the Suitability and Security Clearance Performance Accountability Council (PAC) to convene a task force to examine the policies and procedures that determine level of access to CHRI for background investigations. The task force determined that the federal government and national security would benefit from:

- Improvements in CHRI acquisition through the clarification/modernization of 5 U.S. Code Sec. 9101, the federal regulations that govern access to criminal history records for national security purposes.
- Strengthening education of the law enforcement and federal background investigator community.
- Allocating funds for dedicated resources and technical system improvements.

These recommendations help guide LELO's role in developing policy, training, networking, and relationship building with our state and local law enforcement partners.

Established in April 2017, LELO focuses in part on educating state, local, tribal, and territorial law enforcement agencies on 5 USC 9101 and the process by which agencies disseminate CHRI. The office is led by a federal program manager and branch chief, who focus on developing strong relationships with the law enforcement community through outreach, training, and networking opportunities. These efforts help LELO improve cooperation, encourage the accurate and timely collection of CHRI, and in turn, reduce national security risks.

Currently, LELO engages regularly with many of the nation's 18,000 law enforcement agencies and another 26,000 courts and criminal justice entities. However, some of these agencies are non-compliant. LELO maintains a database of non-compliant law enforcement agencies that are deficient in staffing, resources, and/or lack knowledge to comply with the federal requirements. LELO utilizes this information to concentrate on outreach, agency education, federal grants, and product improvement to decrease the number of non-compliant agencies. More specifically, LELO is set to hire the first two of what is expected will be a half dozen or more specialists to work directly in the field with law enforcement agencies in areas of the country where the need for engagement is particularly acute.

As DCSA is the lead federal Investigation Service Provider (ISP), LELO works across the government to establish the standard and lay the foundation for our ISP partners with all federal, state, local, and tribal law enforcement outreach efforts. The office continues to expand, while looking for new ways to forge relationships and effectively collect CHRI data in support of background investigations and national security.

DCSA SUPPORTS INDOPACOM THROUGH COLLABORATION AND POTENTIAL THREAT AWARENESS

One of the unique challenges DCSA faces is countering threats to critical defense technologies in overseas locations. Without employees permanently stationed abroad, DCSA relies on personnel at overseas military installations to provide support to cleared contractor employees and the contractor's U.S. home offices to ensure employees are meeting reporting requirements. DCSA also has limited visibility on where programs and personnel are located overseas. These challenges are especially prevalent in the Indo-Pacific region, where vast distances separate cleared contractor employees from their company's security personnel. However, that is changing in the United States Indo-Pacific Command (INDOPACOM), formerly known as Pacific Command (PACOM).

On May 30, 2018, PACOM was renamed INDOPACOM. This change reflects the increasing interconnectivity of the Indian and Pacific Oceans and reinforces the United States' commitment to the safety and security of all nations in the region, especially with the return of great power competition.

The INDOPACOM region is incredibly important. Comprised of 36 nations, it is home to more than half of the world's population. From a military perspective, seven of the largest standing armies are in the region, and the United States is allied with five of them through mutual defense treaties. The region is also a major driver of the global economy, containing nine of the largest ports in the world.

In 2018, the National Defense Strategy committed the United States to maintaining a free Indo-Pacific region. In testimony before the Senate Armed Service Committee in March 2021, INDOPACOM Commander Admiral Philip S. Davidson noted, "The greatest danger for the United States is the erosion of conventional deterrence. Without a valid and convincing conventional deterrent, the People's Republic of China will be emboldened to take action in the region to supplant U.S. interests."

During a recent visit to Singapore, Secretary of Defense Lloyd J. Austin III emphasized that U.S. efforts in the Indo-Pacific will be a whole of government approach with DOD working alongside State Department diplomats, economic experts, and others.

"For decades, we have maintained the capabilities, the presence, and the relationships needed to ward off conflict and to preserve the stability that lies at the heart of our shared prosperity," Austin said. "Yet, emerging threats and cutting-edge technologies are changing the face and the pace of warfare. So, we are operating under a new, 21st century vision that I call 'integrated deterrence.'"

This concept means using every military and non-military tool in lock-step with allies and partners. "Integrated deterrence is about using existing capabilities and building new ones and deploying them all in new and networked ways — all tailored to a region's security landscape, and in growing partnership with our friends," Austin continued.

Davidson noted four key focus areas: increasing joint forces including cyber capabilities, enhancing force design and posture, strengthening allies and partners, and exercising experimentation and innovation amongst allies and partners. Furthermore, Davidson emphasized several technologies such as artificial intelligence, quantum computing, remote sensing, machine learning, big data analytics, and 5G technologies as critical enablers. Charged with oversight of many cleared facilities involved with developing these technologies, DCSA is in a unique position to provide support to INDOPACOM in many areas.

DCSA COUNTERINTELLIGENCE SUPPORT TO INDOPACOM

DCSA has a vital role in ensuring critical defense technology is delivered to the warfighter uncompromised. DCSA Counterintelligence (CI) is working directly with INDOPACOM and its subordinate commands, United States Forces Japan (USFJ) and United States Forces Korea (USFK), to develop new and innovative ways to collaborate in the protection of critical defense technologies. DCSA is doing this by 1) developing and implementing one of the first overseas Research and Development Defense Alliance of the Research Triangle (RED DART) programs, 2) working with Force Protection Detachments (FPD), 3) supporting cleared defense contractors attending conferences, tradeshows, and conventions, 4) and collaborating with our allies in the region.

RED DART PROGRAMS

The RED DART program, first established in South Carolina and North Carolina, has been a critical success within the United States and has provided invaluable support to cleared industry by allowing intelligence and federal law enforcement to share information more effectively. The backbone of the RED DART program is an aggressive CI awareness and education briefing program aimed at cleared contractors. The briefing focuses on bringing real-time, specific, and relevant CI information to industry so they can better protect themselves and their intellectual property.

With the support of USFJ and USFK, the RED DART program is now being implemented at both sub-commands with the goal of partnering CI services with cleared employees to provide coordinated CI support within Japan and Korea. The goal of the RED DART program is to provide local CI- and security-related education and training to cleared contractor employees in Japan and Korea and to act as a local resource for contractor employees in meeting their reporting requirements.

FORCE PROTECTION DETACHMENTS ENGAGEMENT

DCSA is also engaging with the FPDs located in the Indo-Pacific region. The primary mission of FPDs are to detect threats to DOD personnel and in-transit resources overseas without a permanent DOD CI presence. The FPDs can provide limited CI support to contractor employees traveling in their respective countries and help them gain a better understanding of potential threats to personnel and developing technologies. Additionally, DCSA CI collaborates with the FPDs to provide CI support to contractors who are attending conferences, tradeshows, and conventions in the region.

ALLIES

As INDOPACOM is a large area that has a limited U.S. presence in many locations, the United States' five allies are critical to ensuring the safety and security of critical defense technologies and cleared personnel. As DCSA furthers its relationships and information sharing in the region, it will develop a deeper understanding of threats, which is critical to protecting these U.S. and allied technologies.

Critical Technology Protection, Background Investigations, and Counterintelligence all play a critical role in supporting cleared contractors in ensuring critical defense technology is delivered to the warfighter uncompromised. Our support enables INDOPACOM, their sub-commands, and allies to accomplish their mission and ensure that the Indo-Pacific region remains free with open access to trade routes throughout the region.

GET READY FOR THE RULE:

32 Code of Federal Regulation Part 117: National Industrial Security Program Operating Manual or the “NISPOM Rule”

By Larry Pyles
Critical Technology Protection

On February 24, 2021, 32 Code of Federal Regulation Part 117: National Industrial Security Program Operating Manual (NISPOM) went into effect as a federal rule, turning the “NISPOM Rule” into a common phrase of reference.

The NISPOM Rule implements policy, assigns responsibilities, establishes requirements, and provides procedures consistent with Executive Order 12829: National Industrial Security Program, the policy that outlines the protection of classified information that is disclosed to, or developed by, contractors of the U.S. government. It replaces the NISPOM, DOD Manual 5220.22, which has been in place since 2006, and directs cleared industry to implement the requirements no later than six months from its February 24 effective date.

With this six-month implementation period in mind, DCSA promoted the “GET READY FOR THE RULE” campaign to increase awareness of cleared industry’s responsibilities under the NISPOM Rule. DCSA’s Critical Technology Protection (CTP) directorate worked to develop and communicate tools and resources that enable cleared industry under DOD cognizance to successfully implement the NISPOM Rule. To ease the transition, CTP developed and fielded a NISPOM cross reference tool, which allows users to click on a link in the familiar NISPOM DOD 5220.22-M and find its corresponding section in the NISPOM Rule, helping cleared industry and DCSA personnel become better acquainted with the new rule.

Additionally, CTP held webinars to highlight various aspects of the rule. Notably, the NISPOM Rule’s inclusion of Security Executive Agent Directive (SEAD) 3 expands the reporting requirements for all cleared contractors by adding specific activities that may adversely impact continued national security eligibility. A webinar in July outlining new SEAD 3 reporting requirements drew more than 2,700 participants. The webinar focused on facility security officers’ use of the Industrial Security Letter (ISL) to identify what now needs to be reported and how to go about submitting reports. DCSA also held a webinar on senior management official responsibilities under the NISPOM Rule and the importance of their role in self-inspections, as well as a series of recorded video chats designed to ease the transition for industry.

These communication efforts were especially important given that the NISPOM DOD 5220.22-M has served as NISP guidance for protection of classified information by cleared industry for so long. The NISPOM has seen its share of revisions, most recently with Conforming Change 2 in 2016, which required industry to establish insider threat programs with related training, plans, and minimum standards. Industry leaned forward and set the bar by establishing these programs and did so ahead of many federal executive branch agencies.

Like Conforming Change 2, implementing the NISPOM Rule comes with challenges and new requirements, such as SEAD 3 reporting. Industrial security professionals have had to adapt to the format change, going from a manual with numbered paragraphs and sections, to that of a federal regulation. Despite this major change in formatting, cleared industry has been able to pick up the new rule and develop or adopt adaptive measures that allowed them to move forward, and demonstrate their capabilities and adapt when changes or new requirements in the NISP are necessary.

Providing cleared industry with the understanding needed for successful implementation of the NISPOM Rule required a wide range of products, communication activities, and tools, as well as coordination with the Office of the Under Secretary of Defense for Intelligence and Security (OUSD(I&S)) and cleared industry.

DCSA IS HERE TO HELP!

For additional resources, please visit:
https://www.dcsa.mil/mc/ctp/NISPOM-Rule/

CONTROLLED UNCLASSIFIED INFORMATION (CUI) PLANNING: STRATEGIC INSIGHTS

By John B. Massey
Critical Technology Protection

Government and industry security professionals may look at the Controlled Unclassified Information (CUI) program and think it's just another requirement to be met and even more unchartered waters to navigate through. To overcome this perception, it's important to understand the why behind the program and how U.S. government and industry must collectively work together to meet the spirit and the intent of the CUI program, protect information that warrants protection, and prevent unauthorized disclosure of information requiring special safeguarding. CUI is the path of least resistance for adversaries and the aggregation of CUI can become just as valuable, if not more valuable for adversaries as information found in classified settings. Adversaries change their tactics, and we must as well. The time to protect certain categories of information that warrant protection is now.

> ***"The current threat environment challenges the United States' ability to secure its workforce, operations, and position as a world leader."***
>
> — Defense Security Enterprise Strategy 2021-2025

The CUI program can be traced back to November 4, 2010, when former President Barack Obama signed Executive Order (EO) 13556, establishing an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies. This EO was signed as a result of inconsistent marking and safeguarding of documents and ad hoc, agency-specific policies and procedures. A decade later, on March 6, 2020, DOD Instruction (DODI) 5200.48 was released, establishing policy, assigning responsibilities, and prescribing procedures for CUI throughout the DOD.

DODI 5200.48 directed DCSA with eight responsibilities related to CUI. These responsibilities can be broadly categorized into two general buckets: program administration and assessment of contractor compliance. The program administration role includes administering the DOD CUI Program for contractually established CUI requirements for contractors in classified contracts, providing security education, training, and awareness on CUI-related topics, and providing security assistance and guidance to DOD components on the protection of CUI. This bucket further requires the establishment of threat notification and unauthorized disclosure processes and serving as the lead for the latter. Additionally, DCSA will play a lead role in coordinating with the DOD Chief Information Office (CIO) to implement uniform security requirements for National Industrial Security Program (NISP) contractors and efforts to consolidate DOD component input on the oversight of CUI protection requirements in DOD classified contracts for NISP contractors. Fulfilling these responsibilities is critical to ensuring the success of the DOD CUI Program.

SECURITY EDUCATION, TRAINING, AND ASSISTANCE

DCSA the premiere provider of security education and training, and one of DCSA's biggest tasks with respect to CUI is providing security education, training, and awareness on CUI-related topics. DCSA succeeds in its core mission areas as a result of the assistance, expertise, and guidance agency personnel provide to industry on a routine basis. This includes, but is not limited to, providing contractors with guidance on reporting requirements, assisting industry to ensure classified information is adequately safeguarded, supporting industry's conduct of administrative inquiries into security violations, and working collaboratively with industry partners on the submission of facility clearance documentation. Whether it be through advice and assistance or sharing with industry the training and resources available to build and sustain security programs, these efforts strengthen relationships and enable government and industry partners to proactively manage their security programs.

Some CUI security education, training, and awareness resources and products already exist, but DCSA will play a vital role in identifying and developing new training, resources, job aids, and tools to enable industry's success and support DOD partners. As a part of those efforts, the CTP team is engaging with DOD and industry partners to share best practices, lessons learned, and work collaboratively to develop resources that are simple, easy to understand, and easy to use. This is not a one-time effort, and it will be absolutely critical to develop a repository of products and tools for DOD and industry to use in support of their CUI programs.

While DCSA's role is limited to the DOD CUI Program and primarily NISP contractors, I view the agency's responsibilities and the initial efforts we have taken as an opportunity to be a government-wide leader in the CUI mission space. Several years ago, when DOD, non-DOD agencies, and industry were all working towards establishing and maturing insider threat programs, DCSA (then DSS) stepped up as a leader and played a pivotal role in assisting the broader community in making it to shore. DCSA has an opportunity to play a similar role with CUI and doing so successfully will support consistency and standardization with how CUI is protected throughout DOD, the broader U.S. government, and industry.

> ***"The United States faces an unprecedented threat environment as asymmetric, non-kinetic warfare increasingly threatens critical infrastructure, undermines democratic institutions, and erodes U.S. military readiness and competitive advantage."***
>
> — Defense Security Enterprise Strategy 2021-2025

PROCESS DEVELOPMENT

DCSA will also play a vital role in establishing and maintaining a threat notification process and serving as the DOD lead to report unauthorized disclosures of CUI. There are several categories of information which may constitute CUI. From critical infrastructure information to certain defense, financial, and export controlled data, categories of information contained in the CUI Registry may not rise to the level of being classified, but they do warrant additional protection and safeguarding. If this type of information is disclosed to an unauthorized recipient, steps must be taken to ensure further disclosure does not occur. Moreover, threats may exist to certain categories of CUI, which may warrant notification to DoD components and industry contractors. DCSA is tasked with taking a lead role in developing both of these processes and both will be critical to the comprehensive administration of the DOD CUI Program.

COMMUNITY LEADER

DCSA will also provide security assistance and guidance to DOD components on the protection of CUI. This responsibility is specific to when DOD components establish CUI requirements in DOD classified contracts for NISP contractors falling under DCSA security oversight. This responsibility makes DCSA a community leader working with DOD partners to collectively protect CUI resident in cleared industry. This is not a new role for DCSA as the agency has historically worked with DOD partners in protecting classified information and is therefore a natural extension of what the agency already does in the classified domain. A continuous and ongoing outreach effort with DOD component partners will be essential to ensuring the agency adequately fulfills this responsibility as a community leader.

STANDARDIZATION AND CONSISTENCY

Both government and industry alike have expressed concerns about the inconsistencies of CUI requirements in both DOD and non-DOD contracts. Industry, specifically, has voiced concerns about having to prepare to meet different CUI requirements for different customers, using a hodgepodge of solutions to ensure compliance based on individual customer needs.

DCSA has two responsibilities that will support standardization and consistency, at least with respect to CUI requirements in DOD classified contracts. The first is a coordination role with the DOD CIO to implement uniform security requirements for NISP contractors. This provides an opportunity for DCSA to drive consistency at least within DOD. The second is to lead the consolidation of DOD component input on the oversight of CUI protection requirements in DOD classified contracts for NISP contractors. This role is intertwined with DCSA's responsibility to provide security assistance and guidance to DOD components and provides the agency with an opportunity to drive standardization and consistency across the Department, leading to greater uniformity for industry.

While these two responsibilities in DODI 5200.48 are specific in scope to DOD classified contracts and NISP contractors, DCSA has the opportunity to directly support Objective 2.1 of the recently released Defense Security Enterprise Strategy 2021-2025, which calls for standardized coordination among security disciplines and security-related functions. DCSA has an opportunity to support this objective by not only being an enterprise leader within DOD, but driving standardization and consistency across the U.S. government

COMPLIANCE ROLE

The aforementioned responsibilities all fall within CUI program administration, but there remains another critical responsibility for DCSA to exercise in the CUI mission space. That responsibility involves the assessment of contractor compliance with contractually established CUI system requirements in DOD classified contracts associated with the NISP. DCSA's administration of the DOD CUI Program and many of the other responsibilities outlined in DODI 5200.48 directly support the assessment of contractor compliance.

First, DCSA must develop the tools, training, and resources to support industry's development, management, and sustainment of its own internal CUI program. This includes developing those tools that will support industry meeting CUI-related requirements, and resources which provide industry with capabilities to certify that programs are in place and compliant. Much like the responsibility of providing security education, training, and assistance, this is not simply a one-and-done effort and must be evolved and expanded over time.

Will on-site CUI compliance assessments be conducted by DCSA? Not in the near future. Instead, DCSA will lead efforts to build tools and resources to help industry develop, manage, and sustain CUI programs. Further, DCSA will work to make necessary updates to existing information technology systems and the Self-Inspection Handbook to support industry's ability to self-assess CUI compliance and self-attest to DCSA of that compliance. Potential assessments in the future will explore reviewing self-assessments for anomalies, leveraging information technology capabilities and automation, and conducting virtual reviews. DCSA will make efforts to work more rapidly, more efficiently, and reduce and minimize redundant efforts that industry may face with respect to CUI assessments.

CONCLUSION

Developing and building a CUI program for both government and industry is a significant undertaking, but there is no mistake that the need to protect certain categories of information is more important than ever before. Adversaries target this information because, historically, this information has been much more vulnerable and an easier target than information found in classified domains. In many instances, CUI information in the aggregate may become just as valuable, if not more valuable, than information which is classified. It is imperative that DCSA fulfills its eight CUI responsibilities in a methodical, deliberate manner, emplaces the tools and resources necessary to help our partners, and functions as a leader in employing an all-of-government approach to assist both government and industry in collectively navigating these new waters.

VIRTUAL SECURITY CONFERENCE LOOKS TO THE FUTURE OF SECURITY IN DOD

Over August 3-5, DCSA's Center for Development of Security Excellence (CDSE) hosted a three-day virtual security conference for approximately 3,000 registered security professionals from DOD and other federal agencies, continuing a tradition dating back to 2008.

Conference topics and training segments centered around the theme of "Collaborative Resilience: Vision Turns to Reality in Security Today." Topics included National Background Investigative Services (NBIS) and National Industrial Security Program Operating Manual (NISPOM) updates, collaboration peripherals, controlled unclassified information (CUI), extremism, insider threat, expanding foreign ownership, control, or influence (FOCI) requirements, and the future of personnel vetting.

Garry Reid, director for Defense Intelligence, Counterintelligence, Law Enforcement and Security, from the Office of the Undersecretary of Defense for Intelligence and Security (OUSD(I&S)), gave an overarching Defense Security Enterprise (DSE) perspective, including the Department's vision for the next four years. Reid noted that DOD leadership, including Ronald Moultrie, the new Under Secretary of Defense for Intelligence and Security, recognizes the hard work being done in the security mission space. He also cited a number of high visibility security incidents that demonstrate the community's resilience but also serve to elevate the need for a security enterprise positioned to address new, evolving challenges. Reid emphasized that people on the ground are what matters and encouraged attendees to work together to collaborate, innovate, and think with an enterprise point of view to solve problems.

DCSA Director William Lietzau reinforced Reid's message during his remarks and discussed how DCSA is uniquely poised to implement the Department's new security strategy. Lietzau cited the number of training courses offered by CDSE and how important security training is to the enterprise, as it can serve as a defensive capability against attacks and adversaries.

Lietzau then discussed Trusted Workforce 2.0, the whole of government approach to redesigning the personnel vetting process and the DCSA role in implementation. He noted the 10-plus-year investment in the process and how that investment is now close to fruition. On the industrial security side, Lietzau said more needs to be done to bring attention to the mission and improve the agency's capabilities.

Lietzau concluded his remarks by fielding questions from the audience on NBIS, the role of insider threat in personnel vetting, Continuous Vetting (CV), and the status of the Defense Information System for Security (DISS).

The virtual format allowed participation from around the globe and the opportunity for security managers to connect with experts and ask questions in an interactive forum.

DCSA WELCOMES STUDENT HIRES FOR SUMMER 2021

In 2020, DCSA was on track to hold its first summer hire program. However, the DCSA Human Capital Management Office (HCMO) unfortunately had to hit pause due to COVID-19. This year, DCSA Director William K. Lietzau supported a limited scope pilot program, and HCMO launched DCSA's inaugural student program "DCSA Student Experience (DSE)", welcoming 11 new student hires in June 2021.

This year's summer program not only received a new name, but a new focus as well. As a limited pilot, HCMO shifted away from a focus on summer employment to a program aimed at identifying students who, with the right performance and fit, could be non-competitively converted to permanent employees across all mission areas. Hiring managers will monitor and assess work performance and provide students with networking and training opportunities to better understand the DCSA mission and its role in the Intelligence Community.

The DSE aims to provide students with opportunities to gain experience beyond their studies in critical mission areas, including Adjudications, Critical Technology Protection (CTP), Background Investigations, Counterintelligence, DOD Insider Threat Management and Analysis Center (DITMAC), and Vetting Risk Operations (VRO). Each student will showcase their capstone projects agency-wide at the end of the cohort period. Aligned with the DCSA vision, the DSE will help to develop a vibrant pipeline of security and counterintelligence professionals who will be prepared to support the agency's initiatives to safeguard our nation's critical assets.

This year, the program was limited to the National Capital Region (including Fort Meade). Hiring managers and sponsors from these areas assisted HCMO in writing job announcements and interviewing 188 applicants, ultimately choosing 11. HCMO targeted students with special skills and experience at diverse and inclusive educational institutions who were completing their Junior year of college. In addition to traditional job announcements, HCMO highlighted these opportunities on DCSA's social media accounts (LinkedIn, Facebook and Twitter) and alerted numerous colleges and universities.

Upon arrival, students were greeted by a virtual New Student Experience Orientation and also attended a two-week DCSA New Employee Experience (NEX) orientation along with other new employees. While the first two weeks were packed with onboarding activities, HCMO incorporated space for mission area leads to spend "virtual" time with students to provide insights on their roles and responsibilities. This engagement promoted inclusiveness, acculturation, and supported professional development.

DSE student hires have and will continue to participate in periodic virtual Student Exchange Forums as an informal way to discuss current projects, experiences, lessons learned, and provide professional development. These forums are designed to enhance their professional growth within the agency.

To add to the experience, the students also had the opportunity to meet with the DCSA director during an August Brown Bag session. And in mid-August, HCMO hosted a virtual showcase to display the students' capstone projects and celebrate their accomplishments. This year's capstone project asked students to reflect on their experience and other important topics relative to their mission areas. This event officially closed out the DSE cohort.

HCMO will use feedback received from students and supervisors at the end of the program and hopes to expand the program to other mission areas and enabling offices. More information for the summer 2022 program will be available later this fall.

DCSA Director William K. Lietzau answers questions during a brown bag meeting with participants of the DCSA Student Experience. (DOD photo by Christopher P. Gillis)

DEFENSE COUNTERINTELLIGENCE
AND SECURITY AGENCY

27130 Telegraph Road
Quantico, Virginia, 22134

DCSA.pa@mail.mil

571-305-6562

www.DCSA.mil